DESIGN OF A SECURE AND EFFICIENT MULTIPLE COINS PLUS MULTIPLE DENOMINATIONS E-CASH SCHEME

CHANG YU CHENG

UNIVERSITI TEKNOLOGI MALAYSIA

PSZ 19:16 (Pind. 1/97)

UNIVERSITI TEKNOLOGI MALAYSIA

BORANG PENGESAHAN STATUS TESIS◆

JUDUL: DESIGN OF A SECURE AND EFFICIENT MULTIPLE COINS PLUS MULTIPLE DENOMINATIONS E-CASH SCHEME

SESI PENGAJIAN: 2003/2004

Saya CHANG YU CHENG
(HURUF BESAR)

mengaku membenarkan tesis (PSM/Sarjana/Doktor Falsafah)* ini disimpan di Perpustakaan Universiti Teknologi Malaysia dengan syarat-syarat kegunaan seperti berikut:

1. Tesis adalah hakmilik Universiti Teknologi Malaysia.
2. Perpustakaan Universiti Teknologi Malaysia dibenarkan membuat salinan untuk tujuan pengajian sahaja.
3. Perpustakaan dibenarkan membuat salinan tesis ini sebagai bahan pertukaran antara institusi pengajian tinggi.
4. **Sila tandakan (✓)

☑	SULIT	(Mengandungi maklumat yang berdarjah keselamatan atau kepentingan Malaysia seperti yang termaktub di dalam AKTA RAHSIA RASMI 1972)
☐	TERHAD	(Mengandungi maklumat TERHAD yang telah ditentukan oleh organisasi/badan di mana penyelidikan dijalankan)
☐	TIDAK TERHAD	

(TANDATANGAN PENULIS)

Alamat Tetap:
23, JALAN ZABEDAH, 83000 BATU
PAHAT, JOHOR, MALAYSIA

Tarikh: 1 Sept 2004

Disahkan oleh

(TANDATANGAN PENYELIA)

PROF. MADYA DR. JASMY YUNUS
Nama Penyelia

Tarikh: 1/9/2004

CATATAN:
- * Potong yang tidak berkenaan.
- ** Jika tesis ini SULIT atau TERHAD, sila lampirkan surat daripada pihak berkuasa/organisasi berkenaan dengan menyatakan sekali sebab dan tempoh tesis ini perlu dikelaskan sebagai SULIT atau TERHAD.
- ◆ Tesis dimaksudkan sebagai tesis bagi Ijazah Doktor Falsafah dan Sarjana secara penyelidikan, atau disertasi bagi pengajian secara kerja kursus dan penyelidikan, atau Laporan Projek Sarjana Muda (PSM).

UNIVERSITI TEKNOLOGI MALAYSIA

81310 UTM SKUDAI,
JOHOR DARUL TA'ZIM,
MALAYSIA

TELEFON : +607-5533333 Laman Web : www.fke.utm.my TELEFAX : +607-5566272

FAKULTI KEJURUTERAAN ELEKTRIK

RUJUKAN KAMI (OUR REF) :

Librarian
Perpustakaan Sultanah Zanariah
UTM, Skudai
Johor

1 September 2004

Sir,

CLASSIFICATION OF THESIS AS CONFIDENTIAL
- DESIGN OF A SECURE AND EFFICIENT MULTIPLE COINS PLUS MULTIPLE DENOMINATIONS E-CASH SCHEME
CHANG YU CHENG

Please be informed that the above mentioned thesis entitled ***"DESIGN OF A SECURE AND EFFICIENT MULTIPLE COINS PLUS MULTIPLE DENOMINATIONS E-CASH SCHEME"*** be classified as CONFIDENTIAL for a period of three (3) years from the date of this letter. The reasons for this classification are:

(i) It has market value. This is because it can be developed into a product which has demand in the market.
(ii) The theories in this thesis need to be confidential, since there is huge potential for other products to be developed based on the underlying principle discovered in this work.
(iii) Some of the findings in this thesis are in the process of patenting.

Thank you.

Sincerely yours,

Prof Madya Dr. Jasmy Yunus,
Tel : 07-5591551
Fax : 07-5565899

"I hereby declare that I have read this thesis and in my opinion this thesis is sufficient in terms of scope and quality for the award of the degree of Doctor of Philosophy (Electrical Engineering)

Signature : _____

Name of Supervisor I : Prof. Madya Dr. Jasmy Yunus

Date : 1/9/2004

BAHAGIAN A – Pengesahan Kerjasama*

Adalah disahkan bahawa projek penyelidikan tesis ini telah dilaksanakan melalui kerjasama antara _____ dengan _____

Disahkan oleh:

Tandatangan : ..... Tarikh : .....

Nama : .....

Jawatan : .....

(Cop rasmi)

** Jika penyediaan tesis/projek melibatkan kerjasama.*

BAHAGIAN B – Untuk Kegunaan Pejabat Sekolah Pengajian Siswazah

Tesis ini telah diperiksa dan diakui oleh:

Nama dan Alamat Pemeriksa Luar : **Dr. Yi Xun**
School of Computer Science & Mathematics
Victoria University
Melbourne City, Victoria 8001
Australia

Nama dan Alamat
Pemeriksa Dalam I : **Prof. Madya Dr. Sulaiman Bin Mohd Nor**
Fakulti Kejuruteraan Elektrik
UTM, Skudai

Pemeriksa Dalam II : **Prof. Dr. Abdul Hanan Bin Abdullah**
Fakulti Sains Komputer & Sistem Maklumat
UTM, Skudai

Nama Penyelia lain (jika ada) :

Disahkan oleh Penolong Pendaftar di PPS:

Tandatangan : ..... Tarikh : .....

Nama : **GANESAN A/L ANDIMUTHU**

DESIGN OF A SECURE AND EFFICIENT MULTIPLE COINS PLUS MULTIPLE DENOMINATIONS E-CASH SCHEME

CHANG YU CHENG

A thesis submitted in fulfilment of the
requirements for the award of the degree of
Doctor of Philosophy

Faculty of Electrical Engineering
Universiti Teknologi Malaysia

SEPTEMBER 2004

I declared that this thesis entitled "DESIGN OF A SECURE AND EFFICIENT MULTIPLE COINS PLUS MULTIPLE DENOMINATIONS E-CASH SCHEME" is the result of my own research except as cited in the references. The thesis has not been accepted for any degree and is not concurrently submitted in candidature of any other degree.

Signature : 

Name of Candidate : CHANG YU CHENG

Date : 1 Sept 2004

To my father, mother and sisters for their support and encouragement.

ACKNOWLEDGEMENT

This thesis would not have been possible without the guidance, technical assistance and continuous support of my supervisors, not to mention seriously boosting my confidence at times where I needed it most. Firstly, I am profoundly grateful to my supervisor, Dr. Kamaruzzaman Seman who is now in TELEKOM, who gave me the opportunity to work in Electronic Payment System and always supported me. I would like to thank him for his interest in this work and for his insightful comments. My heartiest thank go to another of my supervisor, Prof. Madya Dr. Jasmy Yunus who gave me the right perspective, insightful comments and patience. His constructive suggestions were great source of motivation and guidance to me.

I thank current members and friends in “Advanced Switching Laboratory”, Dr. Hui Seng Kheong, Goh Kheng Teong, Mohd. Waqas and Fakher Eldin. We always had a great and relaxing atmosphere. Finally, I would like also to thank my supervisors, Mr. Goh Chu Leong and UTM for helping me overcome financial concerns and let me focus on my research work. Special thanks to my family for their love and support I always have towards my endeavors.

ABSTRACT

Anonymous electronic cash (E-Cash) are inefficient compared to other electronic payment systems, since the additional "anonymous" functionality increases the complexity and processing time. Thus, the objective of this thesis is to address and improve the efficiency of E-Cash. A Modified Batch Signature Generation Concept has been devised and implemented into Brand's model. The resultant multiple coins scheme proved to be more efficient than many existing schemes. Further efficiency improvement was achieved by implementing pre-processing, on-line and post-processing concept. Then, multiple denominations functionality was added to the scheme which further improved the efficiency. After that, coin tracing and owner tracing functionality has been included using New Indirect Discourse of Proof which is more efficient than previous method. The security analysis has been performed on Brand's model/scheme found some lapses in his scheme such that it is vulnerable to some form of attacks. Since Brand's scheme is the basis of most E-Cash schemes including the scheme developed in this research, this discovery is significant. Improvements were then made to the scheme that has been developed to make it secure from these attacks. The resultant scheme is called Chang's scheme. Comparison of Chang's scheme with other "state of the art" E-Cash schemes showed that Chang's scheme is better, if observed from both efficiency and security perspective.

ABSTRAK

Wang elektronik tanpa identiti (E-Wang) adalah kurang cekap berbanding dengan sistem-sistem pembayaran elektronik yang lain, kerana fungsi tambahan "tanpa identiti" meningkatkan kerumitan dan masa pemprosesan. Maka, objektif tesis ini ialah untuk mempertingkatkan kecekapan E-Wang. Satu Konsep Penghasilan Tandatangan Berkumpulan Terubah telah direka dan dilaksanakan dalam model Brands. Skim syiling berganda yang terhasil terbukti lebih cekap daripada kebanyakan skim yang sedia ada. Peningkatan kecekapan yang selanjutnya telah dicapai dengan melaksanakan kaedah pemprosesan secara sebelum, semasa, dan selepas. Selepas itu, fungsi unit berbagai telah ditambahkan pada skim tersebut dan ini meningkatkan lagi kecekapannya. Selepas itu, fungsi pengesanan duit dan pengesanan pemilik telah diserapkan dengan menggunakan *New Indirect Discourse of Proof* yang lebih cekap daripada kaedah sebelumnya. Analisa keselamatan yang telah dilakukan pada model/skim Brands mendapati beberapa kelemahan dalam skimnya dimana ianya tidak boleh menangkis beberapa jenis serangan. Oleh kerana skim Brands ialah asas pada kebanyakan skim E-Wang termasuk skim yang dibangunkan dalam penyelidikan ini, penemuan ini adalah penting. Pembaikan telah dilakukan pada skim yang telah dibangunkan untuk menjadikan ia kebal terhadap serangan-serangan demikian. Skim yang terhasil dinamakan skim Chang. Perbandingan skim Chang dengan skim-skim E-Wang terkini yang lain menunjukkan skim Chang adalah lebih baik, jika dilihat dari kedua-dua sudut kecekapan dan keselamatan.